Congresso de Segurança da Informação das Fatec

A Importância de Senhas Robustas e Exclusivas na Era da Cibersegurança

The Importance of Robust and Exclusive Passwords in the Cybersecurity Era

Leonardo Rodrigues Oliveira, Fatec Ourinhos, leonardo.oliveira148@fatec.sp.gov.br
Paulo Roberto Galego Hernandes Junior, Fatec Ourinhos, paulo.galego@fatecourinhos.edu.br

Resumo

Este artigo apresenta a busca pelo entendimento da motivação das preferências de escolha dos elementos e identificar os padrões dos usuários cotidianos na criação de suas senhas. Por meio da construção, aplicação e análise de uma pesquisa com utilizadores atuais de palavras-passe, foi factível compreender as escolhas e os padrões. Dessa forma, fez-se possível o desenvolvimento de uma ferramenta de geração de lista de palavras para ataque de força bruta com o objetivo de evidenciar a vulnerabilidade. Em síntese, este estudo encontra e comprova a vulnerabilidade nas criações e padronizações de senhas com evidências claras e busca conscientizar os usuários sobre a relevância de formular senhas robustas e exclusivas.

Palavras-chave: Entropia de senha, Engenharia social, Geração de senhas, Ataque de força bruta, Padronização de senhas

Abstract

This article presents the search for understanding the motivation of choice preferences of the elements and identify the patterns of everyday users when creating their passwords. Through the construction, application and analysis of a survey with current users of passwords, it was possible to understand the choices and defaults. In this way, it If possible, the development of a word list generation tool for brute force attack with the aim of highlighting the vulnerability. In summary, this study finds and proves vulnerability in password creation and standardization with clear evidence and seeks to make users aware of the relevance of formulating robust and unique passwords.

Keywords: Password entropy, Social engineering, Password generation, Brute force attack, Password standardization

1. Introdução

A criação e padronização de senhas são questões de extrema importância na era digital, onde a segurança da informação é constantemente desafiada. Senhas fracas e previsíveis podem expor indivíduos e organizações a riscos significativos, permitindo acesso não autorizado a contas e dados sensíveis. Nesse contexto, a compreensão das vulnerabilidades existentes na criação de senhas torna-se fundamental para o desenvolvimento de estratégias eficazes de proteção.

Este artigo científico tem como objetivo realizar uma pesquisa abrangente para identificar os padrões e vulnerabilidades comumente encontrados na criação e padronização de senhas com o intuito de fundamentar o desenvolvimento de uma ferramenta de geração de lista de palavras para ataque de força bruta. A pesquisa buscará explorar as práticas atuais dos usuários, investigando os elementos mais frequentemente utilizados e as tendências observadas.

A necessidade dessa pesquisa se fundamenta no fato de que muitos indivíduos tendem a utilizar senhas previsíveis, como datas de aniversário, nomes próprios, sequências numéricas simples ou palavras comuns, o que torna suas contas vulneráveis a ataques cibernéticos. Além disso, o uso de senhas repetidas em diferentes sistemas também amplia o risco de comprometimento, uma vez que o acesso a uma senha pode permitir o acesso a várias contas.

Ao identificar esses padrões de criação de senhas e entender a motivação por trás de suas escolhas, será possível além de desenvolver um recurso cibernético de exploração efetivo, também conscientizar os usuários sobre a importância de criar senhas robustas e exclusivas.

A metodologia adotada para alcançar os objetivos propostos envolverá a revisão rigorosa da literatura existente sobre o tema, a realização de uma pesquisa e a análise minuciosa dos dados coletados e com isso identificar, conscientizar os usuários com o objetivo de mitigar esta vulnerabilidade. Foi aplicado questionário online e com uma amostra representativa de usuários, a fim de obter informações abrangentes sobre suas práticas de criação de senhas e identificar possíveis padrões que servirão como base na construção de um programa criador de *wordlists* para uso de ataques de força bruta.

Espera-se que os resultados dessa pesquisa possam contribuir para a mitigação dos riscos associados à criação e padronização de senhas. Além disso, espera-se que essa pesquisa promova a conscientização dos usuários sobre a importância de adotar práticas seguras na criação de senhas, a fim de proteger sua privacidade e informações confidenciais.

2. Referencial Teórico

A criação de senhas é um aspecto fundamental para proteger informações sensíveis e prevenir acessos não autorizados. No entanto, apesar dos avanços tecnológicos e do aumento da conscientização, as vulnerabilidades ainda persistem,representando riscos para indivíduos e organizações.

A sociedade se torna com o passar do tempo mais dependente dos computadores e das redes, devido aos benefícios oferecidos pela alta tecnologia que cresce em enorme escala. Com isso Marciano e Lima-Marques (2006),argumenta que várias formas de ameaças, tanto físicas quanto virtuais, proliferam-se dentro deste universo de conteúdos, que comprometem seriamente a segurança das pessoas e das informações, bem como das transações que envolvem o complexo usuário-sistema-informação. Logo, revelou-se uma preocupação com a administração das informações trocadas entre usuários, em redes de computadores, tornando-se indispensável à adoção de procedimentos que visem à segurança das informações.

Segundo Kissell (2018) o conceito base de uma senha é que ela é privada, sendo algo que apenas você e a entidade na qual a sua conta está registrada (um banco, site, serviço de armazenamento etc.) sabem. Se outra pessoa descobre a sua senha, ela poderá acessar todos os seus dados, e isso pode ser apenas o começo.

De acordo com Roccia (2021) a senha ou palavra-chave consiste em um identificador composto por uma sequência de caracteres. Levando em conta letras minúsculas, maiúsculas e dígitos, existem 56.800.235.584 possibilidades para uma senha padrão de 6 caracteres. Esse número aumenta para 735.091.890.625 se contar com todos os 95 caracteres imprimíveis ASCII. Apesar do grande número de combinações possíveis, senhas são os maiores alvos de ataques, dificultando a criação de uma senha realmente segura.

Outro aspecto em questão de gerenciamento de senhas é o uso da mesma senha para diversas plataformas. Kissell (2018) comenta em seu livro também sobre esta questão

alegando que caso o usuário use a mesma senha para diversos serviços, uma vez a senha descoberta por um atacante malicioso, o estrago é potencializado, pois ele terá acesso a tudo.

No estudo conduzido por Ur et al. (2012), é apresentado que muitos sites costumam integrar um medidor de força de senha ao cadastro de usuários para que estes criem senhas suficientemente seguras. São recomendações comuns desses medidores:

- Tamanho mínimo de 6 caracteres;
- Utilizar letras minúsculas, maiúsculas, dígitos e caracteres especiais;
- Não utilizar o nome de usuário na senha.

Naturalmente, obedecer essas regras adicionam entropia a senha, pois ela terá tamanho suficiente e todos os tipos de caracteres. A rigidez e o modo de apresentação dos medidores também são importantes influências no comportamento dos usuários. Medidores mais lenientes parecem deixar as pessoas relutantes em escolherem uma senha julgada fraca.

No entanto, senhas como ”q1w2e3r4t5”e ”P@ssword1”seriam consideradas fortes, mesmo sendo umas das mais comuns. Portanto, apenas essas dicas não são suficientes. Medidores robustos devem, além de assegurar bons tamanho e entropia, comparar a senha com dicionários de senhas já vazadas, e também padrões comuns como sequências alfabéticas ou de teclas.

Outro fator que é de suma relevância, é o fato da aprimoração diária, pois segundo Mitnick e Simon (2003) uma empresa pode ter adquirido as melhores tecnologias de segurança que o dinheiro pode comprar, pode ter treinado seu pessoal tão bem que eles trancam todos os segredos antes de ir embora e pode ter contratado guardas para o prédio na melhor empresa de segurança que existe. Mesmo assim essa empresa ainda estará vulnerável. Diante do exposto pelo autor, afirma-se que a segurança empresarial é aperfeiçoada a cada dia, entretanto, ainda se tem um grande problema, porque mesmo com aparatos de ultima geração não se tem total segurança, ou seja, mesmo com os melhores sistemas sempre as empresas estarão vulneráveis a ataques.

Um outro artigo, este publicado no jornal Wiley/Hindawi em 2018 Zheng et al. (2018) discorre sobre um método alternativo para entender a escolha das senhas por parte do usuário. Nesse estudo é feito uma análise utilizando grafos para expor a conexão entre

as senhas de pessoas diferentes nos conjuntos de dados escolhidos. É citado no estudo que os dados estão fortemente entrelaçados, pois há uma grande ligação entre eles. O estudo cita que há um conflito entre a quantidade crescente de senhas e a capacidade de memorização do usuário.

3. Metodologia

Foi adotada a metodologia de pesquisa por meio de um formulário online com o intuito de investigar os elementos utilizados pelos usuários na criação de senhas e desenvolver uma ferramenta de geração de lista de palavras para ataque de força bruta. O formulário foi meticulosamente elaborado para coletar informações sobre os padrões e elementos de criação de senhas utilizados pelos participantes, fornecendo uma ampla variedade de respostas e insights acerca das práticas adotadas pelos usuários.

A fim de assegurar a qualidade e confiabilidade dos dados coletados, os participantes foram incentivados a fornecer respostas precisas e abrangentes acerca de seus hábitos de criação de senhas. A coleta de dados ocorreu exclusivamente por meio desse formulário online, o qual obteve um total de 91 respostas válidas.

Cabe ressaltar que a pesquisa foi aplicada em um público-alvo específico, que foram estudantes da faculdade FATEC Ourinhos e ETEC Jacinto Ferreira de Sá. Essa escolha de público-alvo pode ter influenciado nos resultados obtidos, uma vez que as práticas de criação de senhas podem variar de acordo com a faixa etária, nível de escolaridade e outras características dos usuários.

Posteriormente, os dados coletados foram submetidos a uma análise utilizando técnicas estatísticas e qualitativas, com o intuito de identificar padrões de comportamento e obter informações relevantes para fundamentar o desenvolvimento da ferramenta.

A ferramenta foi construída em linguagem *python* e *bash script*. A escolha das seguintes linguagens se deu pelo motivo de praticidade na hora da construção da ferramenta e a portabilidade da mesma para sistemas operacionais baseados em UNIX.

A lógica da ferramenta de geração é feita a partir de uma fórmula matemática chamada permutação, que é uma técnica de contagem utilizada para determinar quantas maneiras existem para ordenar os elementos de um conjunto finito, sendo assim tornando capaz de gerar todas as maneiras possíveis de um conjunto de strings inseridas e exportando para um arquivo de extensão aceito por recursos de *brute force*.

4. Resultados e Discussões

Os dados apresentados na Figura 1 sugerem uma distribuição significativa de participantes na faixa etária de 15-20 anos, representando a maior porcentagem, de 82,4%, do total de respostas. Isso indica que a maioria dos participantes do formulário se encontra nessa faixa etária.

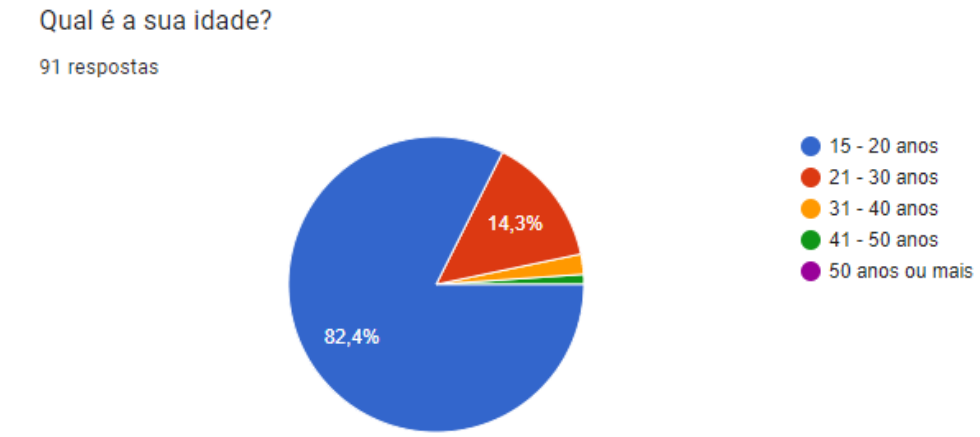

Figura 1. Gráfico 1: Qual a sua idade?

Em contraste, as faixas etárias de 21-30 anos, 31-40 anos e 41-50 anos representam porcentagens menores, indicando uma diminuição gradual na participação dos indivíduos nessas faixas etárias.

Por fim, a faixa etária de 50 anos ou mais não apresenta participantes com base nos dados fornecidos, o que indica uma falta de representatividade nessa faixa etária específica.

Essa análise estatística dos dados de idade fornece uma compreensão básica da distribuição etária dos participantes do formulário, destacando a concentração de respostas na faixa etária mais jovem e a ausência de participantes na faixa etária mais avançada.

Os dados mostrados na Figura 2 permitem observar que uma pequena parcela dos participantes indicou não utilizar elementos relacionados a eles em suas senhas, representando 16,5% das respostas. Isso indica que a menor parte dos usuários não incorpora informações pessoais diretas em suas senhas.

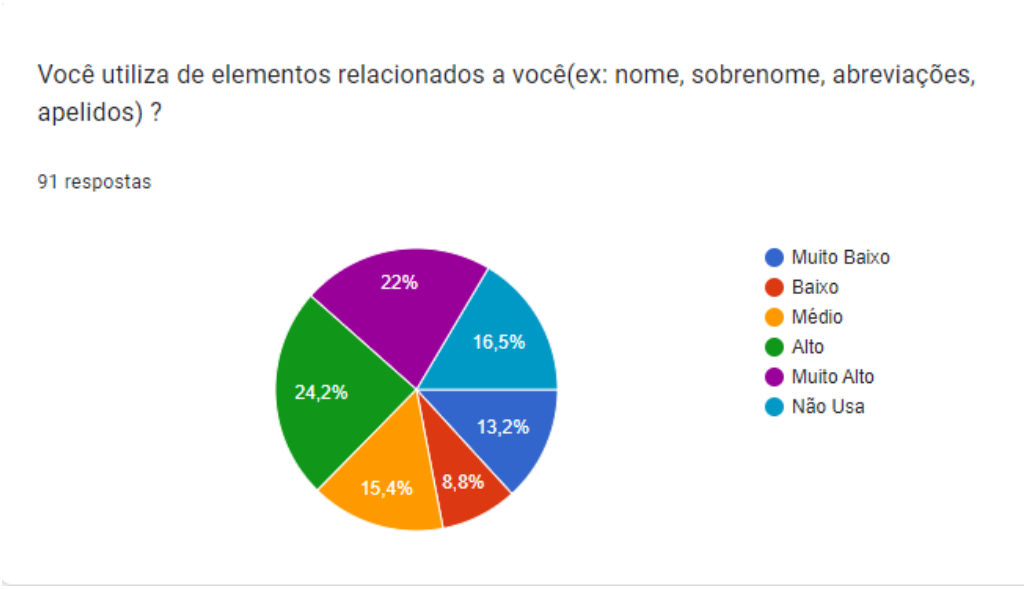

Figura 2. Gráfico 2: Uso do Nome em criação de senhas

Por outro lado, 46,2% dos participantes relataram um nível de uso alto ou muito alto de elementos relacionados a eles, indicando que eles incorporam informações pessoais de forma intensiva em suas senhas. Isso pode representar um risco de segurança, pois senhas que contêm informações pessoais diretas podem ser mais facilmente adivinhadas ou comprometidas.

Conforme ilustrado na Figura 3 percebe-se que cerca de 27,5% dos participantes relataram não utilizar elementos referentes ao aniversário em suas senhas. Isso indica que uma parcela significativa dos usuários opta por incorporar informações relacionadas à data de nascimento em suas senhas, possivelmente reconhecendo os riscos associados a esse tipo de prática.

Cerca de 35,2% dos participantes relataram um uso muito alto ou alto de elementos referentes ao aniversário em suas senhas. Isso sugere que muitas pessoas podem usar informações específicas do aniversário como parte de suas senhas, o que pode aumentar o risco de comprometimento, pois essas informações são mais previsíveis e podem ser facilmente descobertas por atacantes.

Além disso, aproximadamente 11% dos participantes relataram um uso médio de elementos referentes ao aniversário em suas senhas, apontando que eles podem incorporar

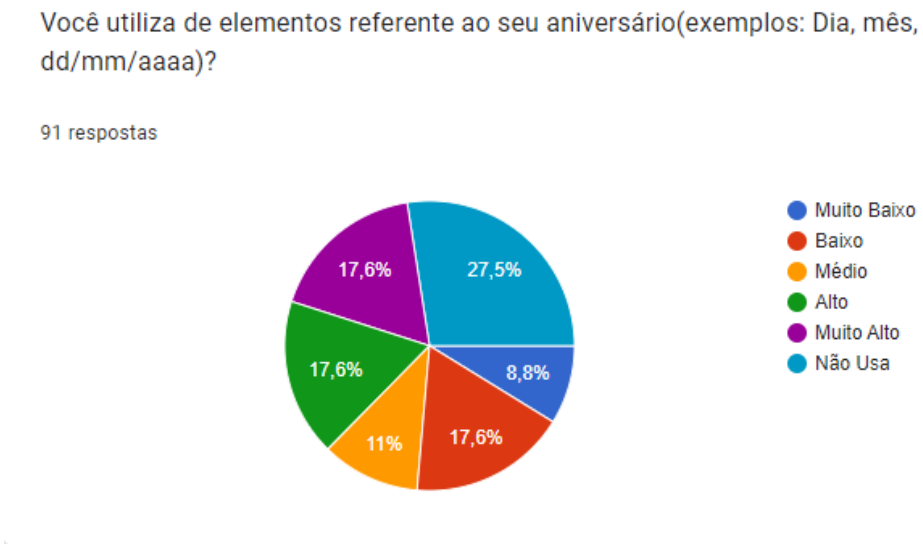

Figura 3. Gráfico 3: Uso de Datas em criação de senhas

algumas informações relacionadas à data de nascimento, mas não de forma intensiva.

Por fim, 8,8% dos participantes relataram um uso muito baixo de elementos referentes ao aniversário em suas senhas. Isso sugere que eles podem usar informações relacionadas à data de nascimento, mas de maneira limitada ou combinada com outros elementos.

Analisando os dados da Figura 4 nota-se que uma parcela significativa dos participantes, cerca de 48,4% relatou não utilizar elementos referentes ao número de telefone em suas senhas, prenunciando que a maioria dos usuários evita incorporar seu número de telefone como parte de suas senhas, reconhecendo os riscos associados a esse tipo de prática.

Em relação aos níveis de uso, os resultados mostram uma distribuição variada. Apenas 12,1% dos participantes relataram um uso alto ou muito alto de elementos relacionados ao número de telefone em suas senhas, indicando que eles incorporam essas informações de forma intensiva.

De outro lado, cerca de 38,5% dos participantes relataram um uso baixo ou muito baixo de elementos relacionados ao número de telefone, indicando que eles podem usar essas informações, mas de maneira limitada.

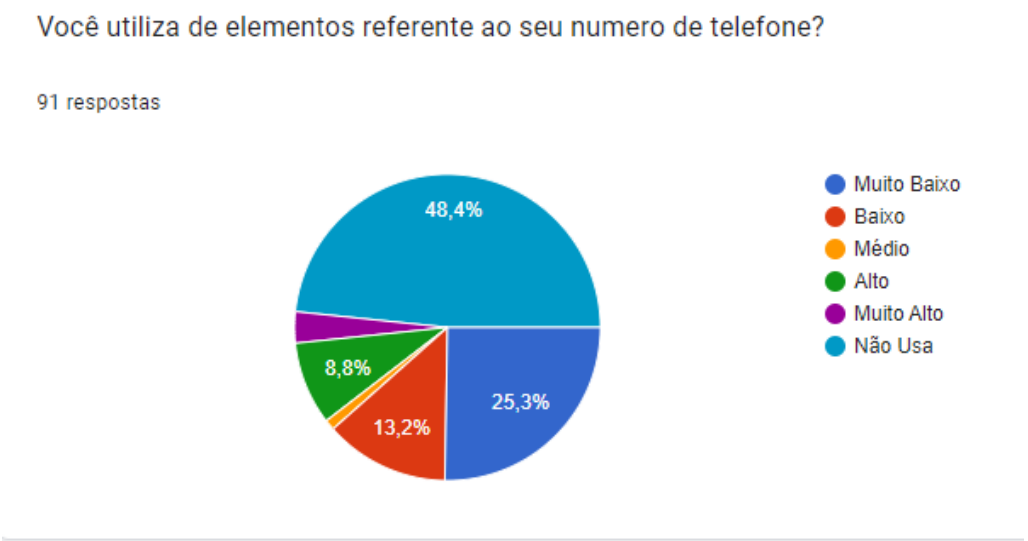

Figura 4. Gráfico 4: Uso de Telefones

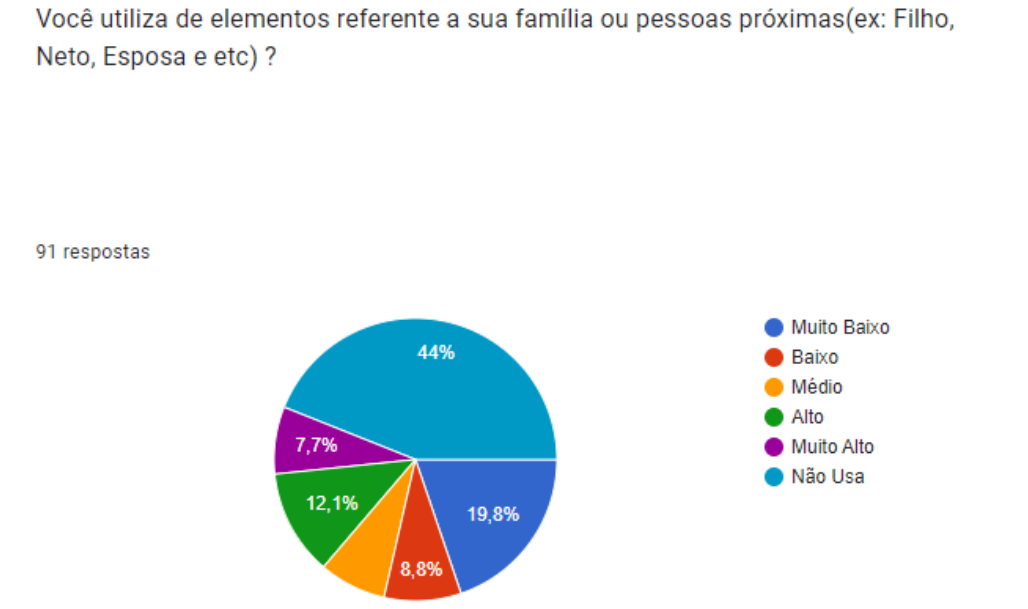

Figura 5. Gráfico 5: Uso de informações referente a família

O gráfico apresentado na Figura 5 moestra que uma parcela significativa dos participantes, aproximadamente 44%, relatou não utilizar elementos relacionados à família ou pessoas próximas em suas senhas. Isso retrata que a maioria dos usuários evita incorporar relações pessoais em suas senhas, provavelmente reconhecendo os riscos de segurança associados a tais práticas.

Em termos de níveis de uso, os resultados mostram uma distribuição variada. Cerca de 19,8% dos participantes relataram um uso alto ou muito alto de elementos relacionados à família ou pessoas próximas em suas senhas, sugerindo que eles incorporam essas informações de forma extensiva.

Por outro ângulo, 38,6% dos participantes relataram um uso baixo ou muito baixo, sugerindo que eles utilizam essas informações de forma limitada em suas senhas.

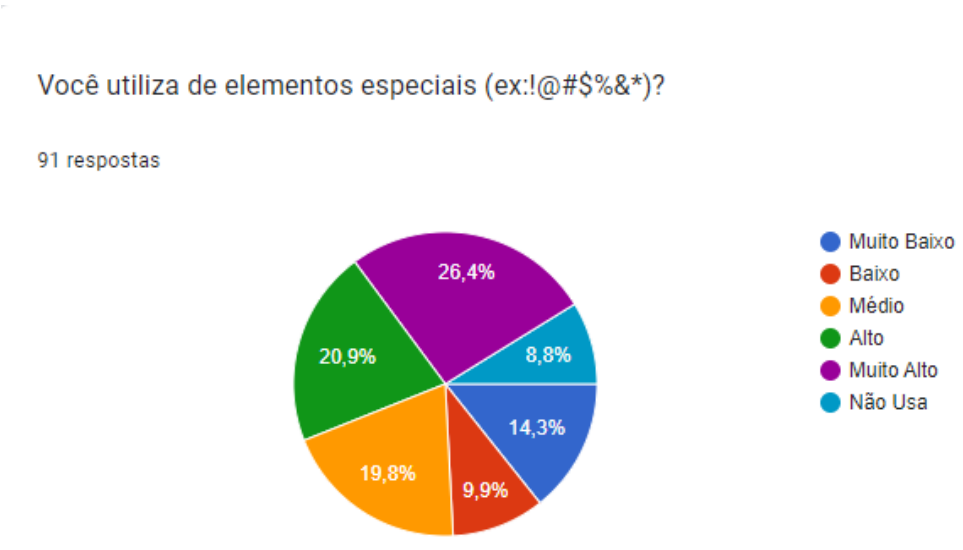

Figura 6. Gráfico 6: Uso de elementos especiais na criação de senhas

Observando os dados apresentados na Figura 6, vê-se que uma parcela significativa dos participantes, aproximadamente 47,3%, utiliza elementos especiais em suas senhas em um nível alto ou muito alto. Isso indica que eles incorporam caracteres especiais, como "!@#$%&*", com frequência e de forma abrangente.

Por outra perspectiva, aproximadamente 19,8% dos participantes relataram um uso médio de elementos especiais. Isso aponta que eles incorporam esses caracteres de

forma moderada em suas senhas.

Em contrapartida, 9,9% dos participantes relataram um uso baixo de elementos especiais, sugerindo que eles utilizam esses caracteres de forma limitada em suas senhas.

Adicionalmente, 14,3% dos participantes relataram um uso muito baixo de elementos especiais.Significando que eles raramente ou quase nunca utilizam esses caracteres em suas senhas.

E no fim, cerca de 8,8% dos participantes relataram não utilizar elementos especiais em suas senhas. Demonstrando uma preferência por senhas mais simples, sem o uso de caracteres especiais.

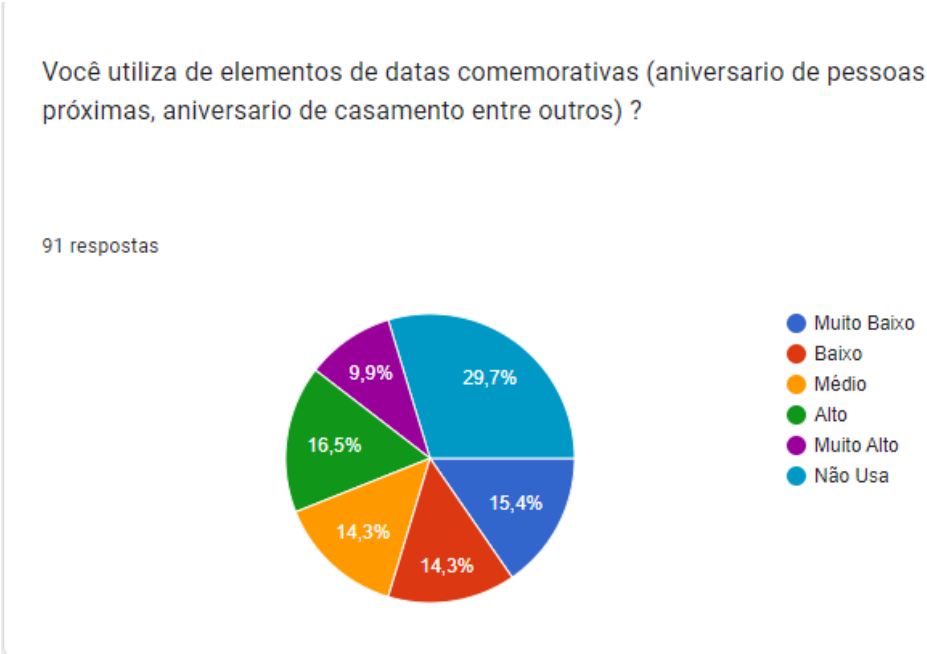

Figura 7. Gráfico 7: Uso de datas comemorativas de terceiros na criação de senhas

Constata-se pelos dados apresentados na Figura 7 que aproximadamente 26,4% dos participantes relataram um uso alto ou muito alto de elementos de datas comemorativas em suas senhas. Expressando que eles incorporam aniversários de pessoas próximas, aniversários de casamento e outras datas especiais de forma frequente e extensiva.

De outro lado, aproximadamente 14,3% dos participantes relataram um uso médio e a mesma quantidade uso baixo de elementos de datas comemorativas. Isso significa que

eles incorporam essas datas de forma moderada ou limitada em suas senhas.

Junto a isso, 15,4% dos participantes relataram um uso muito baixo de elementos de datas comemorativas. Demonstrando que eles raramente ou quase nunca utilizam essas datas em suas senhas.

Por fim, cerca de 29,7% dos participantes relataram não utilizar elementos de datas comemorativas em suas senhas. Isso pode indicar uma preferência por senhas que não estão relacionadas a eventos especiais ou datas significativas.

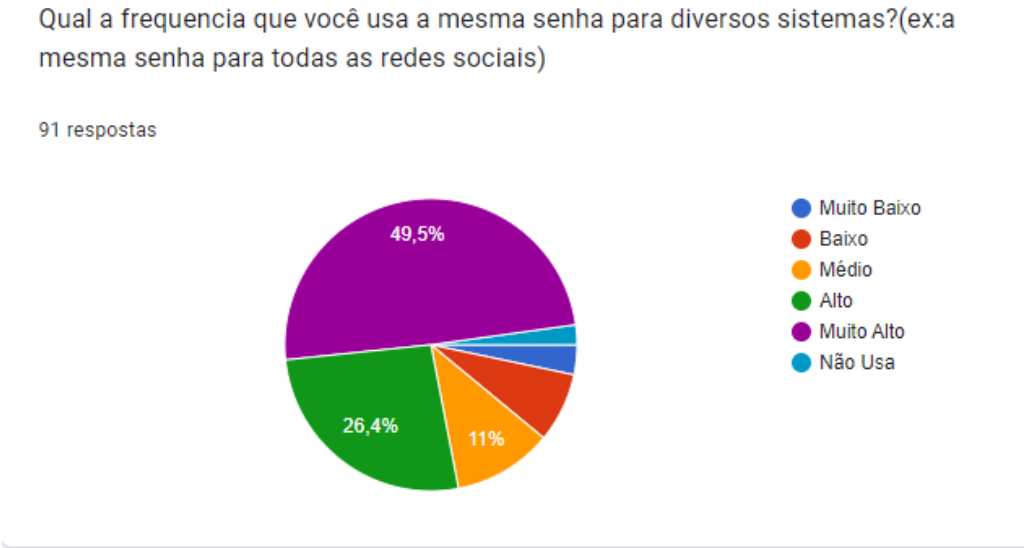

Figura 8. Gráfico 8: Frequência de reutilização de senhas

Ao observar os dados mostrados na Figura 8, identifica-se que cerca de 75,9% dos participantes relataram um uso muito alto da mesma senha para vários sistemas. Pre-nunciando que eles tendem a utilizar uma única senha para todas ou a maioria das suas contas, o que pode representar um risco significativo de segurança. Caso a senha seja comprometida em um sistema, todas as outras contas ficam vulneráveis.

De outra perspectiva, cerca de 11% dos participantes relataram uma frequência média de uso da mesma senha para diversos sistemas. Isso indica que eles ocasionalmente reutilizam senhas, mas ainda fazem esforços para diversificar suas senhas em diferentes contas.

Aproximadamente apenas 11% dos participantes relataram um uso baixo ou muito

baixo da mesma senha para vários sistemas. Isso sugere que eles conscientemente evitam reutilizar senhas com frequência, priorizando a segurança de suas contas.

Finalmente, apenas 2,2% dos participantes relataram não usar a mesma senha para diversos sistemas. Esses indivíduos demonstram uma prática exemplar de segurança, pois reconhecem a importância de utilizar senhas diferentes para cada conta, reduzindo assim o risco de comprometimento múltiplo.

4.1. Script gerador de senhas

Baseado no resultado da pesquisa, foi desenvolvido um script como prova de conceito, cujo objetivo é gerar uma lista de possíveis senhas para um usuário a partir de dados pessoais inseridos por um atacante, com informações pessoais da vítima.

4.1.1. Demonstração

A Figura 9 é uma demonstração de uso da ferramenta com dados de um usuário fictício , onde preenchemos as requisições do programa com dados sem ligação alguma com uma pessoa real.

Figura 9. Demonstração de Uso da ferramenta

Ao inserirmos os dados pessoais, nesta ocasião nome e data de nascimento, um comprimento de máximo de caracteres por combinação de 12 e o nome do arquivo

*w*ordlistjoao.txt, obtemos um retorno do gerador indicando o exito na criação da lista de palavras.

A Figura 10 retrata uma amostra do resultado do funcionamento da ferramenta. Com o uso do comando *cat* para a exibição do conteúdo gerado dentro do arquivo *w*ordlistjoao.txt, é possível observar como as combinações são geradas.

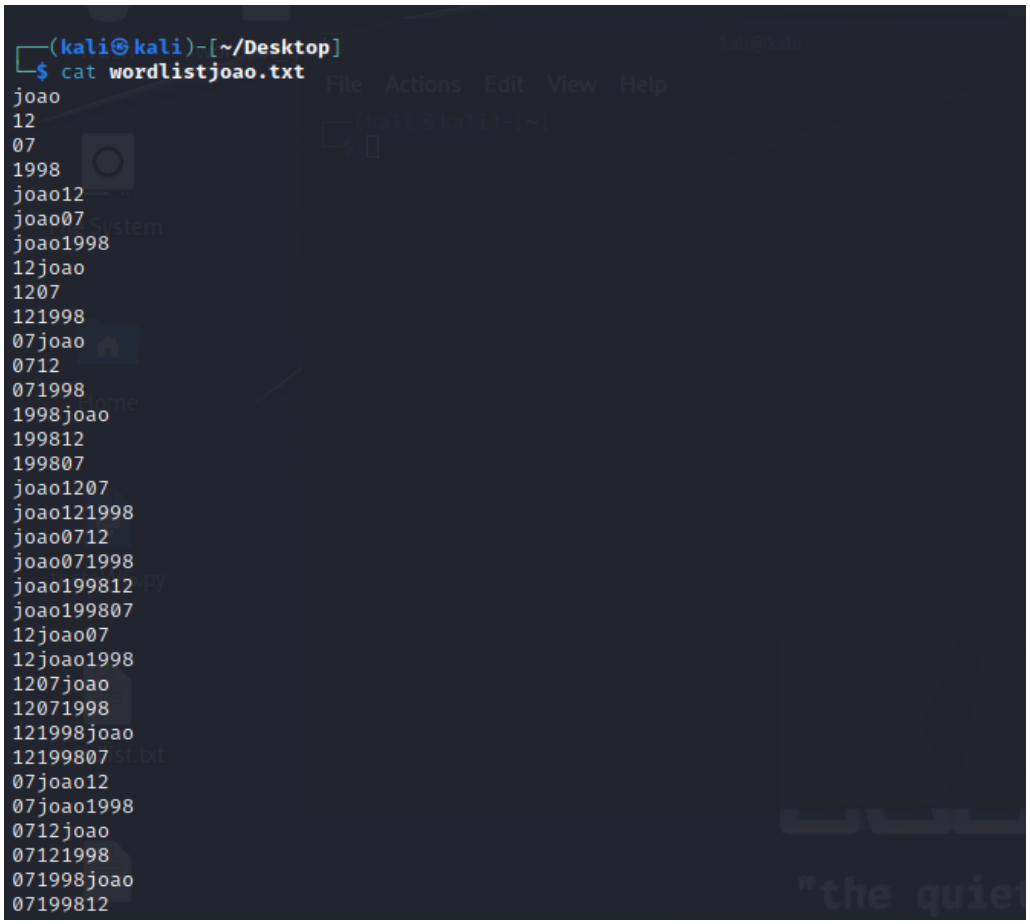

Figura 10. Amostra de Resultado

A Figura 11 apresenta uso do comando *wc* (Word Count) com o parâmetro *-l* para uma contagem de combinações geradas.

Ao analisarmos o funcionamento e o resultado da ferramenta, podemos concluir que o conceito indagado no estudo é verdadeiro, pois na situação hipotética onde o usuário criasse sua senha com os elementos pessoais nome e data de nascimento a sua senha seria descoberta.

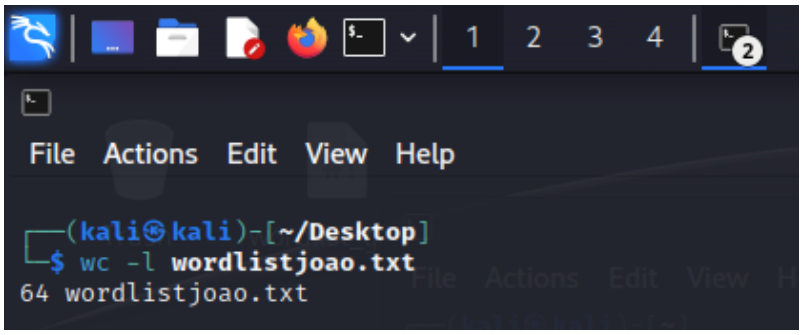

Figura 11. Contagem de Combinações Geradas

5. Conclusão

Após uma análise de todo o estudo realizado, pode-se concluir que a criação e padronização de senhas com elementos relacionados ao usuário ainda são consumidas até o momento. Isso auxilia na presença de vulnerabilidades significativas, como o ataque de força bruta.

Ainda é importante destacar a falha dos usuários em usar a mesma combinação de caracteres para mais de um serviço, tornando o prejuízo expressamente maior. Em uma situação hipotética em que a senha é quebrada, o atacante tem acesso a todos os serviços onde a senha está vinculada como credencial de acesso.

Com isso, pode-se afirmar que, para mitigar esses riscos, é essencial que os usuários adotem práticas seguras na criação de senhas, como a utilização de combinações complexas de caracteres, incluindo letras maiúsculas e minúsculas, números e símbolos especiais. Além disso, é fundamental evitar o uso de informações pessoais óbvias, como nomes, datas de aniversário e números de telefone.

A conscientização dos usuários sobre a importância de criar senhas robustas e exclusivas é um ponto crucial na proteção de suas informações e privacidade. As organizações também têm responsabilidade em fornecer orientações claras e promover a educação dos usuários para evitar ameaças como *phishing* e engenharia social.

A realização de pesquisas abrangentes, como a proposta, permite identificar os padrões de criação de senhas mais comuns e compreender as motivações por trás dessas escolhas. Essas informações são valiosas tanto para o desenvolvimento de estratégias eficientes de segurança quanto para a conscientização dos utilizadores e organizações de

serviços onde a privacidade de segurança depende de identificadores únicos.

Foi possível perceber que, com o uso de um script gerador de *wordlist* a partir de dados pessoais obtidos na Internet ou em Redes Sociais por parte de um atacante, pode-se chegar à senha de um usuário que utiliza senhas fracas e, a partir de um ataque de força bruta, comprometer as contas do alvo.

A proteção efetiva de contas e informações sensíveis requer a adoção de medidas preventivas por parte dos usuários, a implementação de sistemas de autenticação multifator e a constante atualização e fortalecimento das práticas de segurança. Somente assim é possível mitigar os riscos associados à criação e padronização de senhas, garantindo a proteção adequada de dados e a privacidade dos usuários.

Para futuros projetos, sugere-se a aplicação da metodologia de pesquisa em um público-alvo de faixa etária mais elevada, a fim de comparar os resultados obtidos com os resultados d. Essa comparação permitiria verificar se as práticas de criação de senhas variam de acordo com a faixa etária dos usuários e se há diferenças significativas entre os padrões de criação de senhas de diferentes grupos etários. Além disso, seria interessante investigar se há diferenças na percepção de segurança entre os diferentes grupos etários e se isso influencia as práticas de criação de senhas. Para a realização dessa pesquisa, seria necessário adaptar o formulário online utilizado na pesquisa anterior para atender às características do novo público-alvo e garantir a qualidade e confiabilidade dos dados coletados.

Referências

KISSELL, J. *Aprendendo a proteger suas senhas*. [S.l.]: Novatec Editora, 2018.

MARCIANO, J. L.; LIMA-MARQUES, M. O enfoque social da segurança da informação. *Ciência da Informação*, SciELO Brasil, v. 35, p. 89–98, 2006.

MITNICK, K. D.; SIMON, W. L. A arte de enganar. *São Paulo*, 2003.

ROCCIA, R. D. *Usuários respeitam as normas de criação de senhas seguras? Uma análise de datasets de senhas vazadas*. 51 f. Monografia (Monografia) — Instituto de Matemática e Estatística - USP, São Paulo, 2021.

UR, B. et al. How does your password measure up? the effect of strength meters on password creation. In: *21st USENIX Security Symposium (USENIX Security 12)*. Bellevue, WA: USENIX Association, 2012. p. 65–80. ISBN 978-

931971-95-9. Disponível em: ⟨https://www.usenix.org/conference/usenixsecurity12/technical-sessions/presentation/ur⟩.

ZHENG, Z. et al. An alternative method for understanding user-chosen passwords. *Security and Communication Networks*, Hindawi Limited, v. 2018, p. 1–12, 2018.